draft-hujun-idr-bgp-ipsec-01 draft-hujun-idr-bgp-ipsec-transport-mode-00

Hu Jun, Nokia

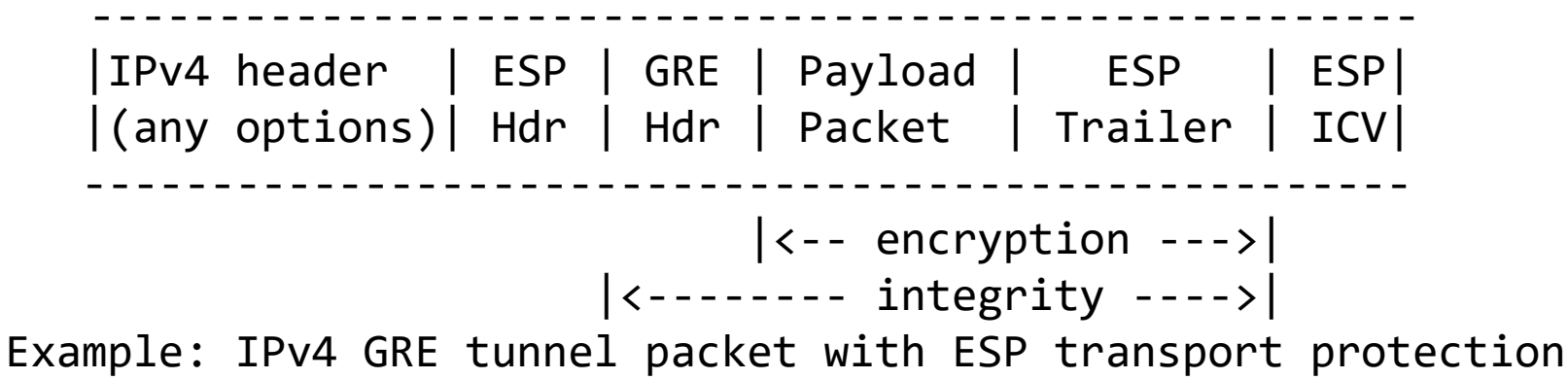
IETF 106

Updates in draft-hujun-idr-bgp-ipsec-01

- replaces color sub-TLV with a new IPsec configuration tag sub-TLV
- add rule on selecting TLV when there multiple feasible TLVs in section (#operation)
- change crypto used in example of section (#operation)
- change title from "BGP Signaled IPsec Tunnel Configuration" to "BGP Provisioned IPsec Tunnel Configuration"
- Add a section (#operationspecifics) on some operation specifics
- add more content in (#security)
- add specification of number of time each new sub-TLV allowed in a given tunnel TLV
- add clarification in section (#intro) to clarify IPsec tunnel means IPsec tunnel mode
- traffic selector protocol and port range now come from tag mapped configuration

draft-hujun-idr-bgp-ipsec-transport-mode-00

- This draft defines a method to advertise IP tunnel encapsulation with IPsec transport mode protection in BGP; e.g GRE with IPsec transport mode, VXLAN with IPsec transport mode ..etc



Example: IPv4 GRE tunnel packet with ESP transport protection

IP Tunnel with IPsec Transport Mode

- Unlike IPsec tunnel mode, which is essentially encapsulate whole IP packet as an payload of a new IPsec tunnel packet, IPsec transport mode does not introduce any new IP header, so it is not a tunnel stack as in “X in Y” type;
- Due to this is the reason, IP tunnel with IPsec transport mode doesn’t fit in current spec of ietf-idr-tunnel-encaps, an extension is needed, draft-hujun-idr-bgp-ipsec-transport-mode-00 is proposed to address such use case;

How does it work?

- A new IPsec Transport Protected sub-TLV is introduced, its value
  its value is a IPsec configuration tag as defined in hujun-idr-bgp-ipsec.
- When an IP tunnel encapsulation TLV include this new sub-TLV, it means advertising router requires IPsec transport mode protection for the corresponding IP tunnel, using the IPsec config as following:
  - ESP transport mode
  - private and public routing instance is same as routing instance in which the packet to be forwarded
  - peer tunnel address is same as indicated by Remote Endpoint sub-TLV
  - local traffic selector:
    - address range: local tunnel endpoint address
    - protocol: tag mapped configuration
    - port range: tag mapped configuration
  - remote traffic selector:
    - address range: address in Remote Endpoint sub-TLV of selected tunnel encapsulation TLV
    - protocol: tag mapped configuration
    - port range: tag mapped configuration
  - its transform and other configuration maps to the tag indicated in the IPsec configuration tag sub-TLV

WG Adoption

As extensions of WG draft ietf-idr-tunnel-encaps, I propose to adopt both draft-hujun-idr-bgp-ipsec and draft-hujun-idr-bgp-ipsec-transport-mode